I Claim:

1. A packet switching controller comprising:

an input for receiving a packet;

a policing element for classifying the packet into a plurality of policeable groups,

wherein the packet is compared against one or more bandwidth contracts defined for the policeable groups to produce one or more policing results.

2. The packet switching controller of claim 1 wherein the policing element includes a policing database, a first policeable group identifier is applied to the policing database to retrieve first policing data and a second policeable group identifier, the first policing data is applied to produce a first policing result, the second policeable group identifier is applied to the policing database to retrieve second policing data, and the second policing data is applied to produce a second policing result.

3. The packet switching controller of claim 1 further comprising a disposition engine for making a disposition decision for the packet, wherein the policing results include one or more disposition recommendations, and the disposition engine uses the policing results and at least one other disposition recommendation to make the disposition decision for the packet.

4. The packet switching controller of claim 1 wherein the policing results are combined into a single result by taking a worst case policing result.

5. A method of processing a packet using a policing element, the method comprising the steps of:

receiving the packet;

classifying the packet into a plurality of policeable groups; and

comparing the packet against one or more bandwidth contracts defined for the policeable groups to produce one or more policing results.

6. The method of processing a packet of claim 5 wherein the policing element includes a policing database, and the method further comprises the steps of:

applying a first policeable group identifier to the policing database to retrieve first policing data and a second policeable group identifier;

producing a first policing result using the first policing data;

applying the second policeable group identifier to the policing database to retrieve second policing data; and

producing a second policing result using the second policing data.

7. The method of processing a packet of claim 5 wherein the policing results include one or more disposition recommendations, and the method further comprises the step of making a disposition decision for the packet using the policing results and at least one other disposition recommendation.

8. The method of processing a packet of claim 5 further comprising the step of combining the policing results into a single result by taking a worst case policing result.

9. A method for policing a data packet received by a data communication switch, the method comprising:

classifying the data packet into a plurality of policeable groups;

identifying policing data associated with one or more policeable groups;

applying the policing data to produce one or more policing results for the policeable groups; and

recommending a disposition of the data packet from the policing results.

10. The method of claim 9 wherein a particular policeable group identifies a type of application to be policed.

11. The method of claim 9 wherein the policing data includes information on bandwidth constraints specified for at least one policeable group.

12. The method of claim 9 wherein the policing results indicate whether the data packet is to be forwarded.

13. The method of claim 9 wherein the policing results indicate whether the data packet is eligible to be dropped.

14. The method of claim 9 wherein the policing results indicate whether the data packet is to be dropped.

15. The method of claim 9 wherein the step of recommending a disposition comprises the step of combining the policing results to make a recommendation.

16. The method of claim 9 wherein the step of recommending a disposition comprises selecting one of the policing results as the recommended disposition.

17. The method of claim 9 further comprising the step of updating the policing data based on the recommended disposition.

18. A method for policing a data packet received by a data communication switch, the method comprising the steps of:

creating a policing database including a plurality of policing data entries specifying policing data for a plurality of policeable groups;

applying a first identifier for retrieving a first policing data associated with a first policeable group and a second identifier identifying a second policeable group;

applying the first policing data to produce a first policing result;

applying the second identifier for retrieving a second policing data;

applying the second policing data to produce a second policing result; and

recommending a disposition of the data packet from the first and second policing results.

19. The method of claim 18 wherein a particular policeable group identifies a type of application to be policed.

20. The method of claim 18 wherein the policing data includes information on bandwidth constraints specified for the policeable group.

21. The method of claim 18 wherein the policing results indicate whether the data packet is to be forwarded.

22. The method of claim 18 wherein the policing results indicate whether the data packet is eligible to be dropped.

23. The method of claim 18 wherein the policing results indicate whether the data packet is to be dropped.

24. The method of claim 18 wherein the step of recommending a disposition comprises the step of combining the first and second policing results to make a recommendation.

25. The method of claim 18 wherein the step of recommending a disposition further comprises selecting either the first or second policing result as the recommended disposition.

26. The method of claim 18 further comprising the step of updating the first or second policing data based on the recommended disposition.

27. A policing engine for a data communication node, wherein the policing engine classifies a packet into a plurality of policeable groups, and wherein the packet is compared for the respective ones of the policeable groups against respective ones of bandwidth contracts to produce respective ones of policing results.

28. A policing engine for a data communication node,

wherein a first policeable group identifier is applied to a policing database to retrieve first policing data and a second policeable group identifier, wherein the first policing data is applied to produce a first policing result, and the second policeable group identifier is applied to the policing database to retrieve second policing data, wherein the second policing data is applied to produce a second policing result.

29. A packet processor comprising:

an input for receiving a packet;

policing means for classifying the packet into a plurality of policeable groups,

wherein the packet is compared against one or more bandwidth contracts defined for the policeable groups to produce one or more policing results.

30. The packet processor of claim 29 wherein the policing means include a policing database, a first policeable group identifier is applied to the policing database to retrieve first policing data and a second policeable group identifier, the first policing data is applied to produce a first policing result, the second policeable group identifier is applied to the policing database to retrieve second policing data, and the second policing data is applied to produce a second policing result.

31. The packet processor of claim 29 further comprising a disposition means for making a disposition decision for the packet, wherein the policing results include one or more disposition recommendations, and the disposition means use the policing results and at least one other disposition

recommendation to make the disposition decision for the packet.

32. The packet processor of claim 29 wherein the policing results are combined into a single result by taking a worst case policing result.